"हिंदी भाषा राष्ट्र निर्माण में सहायक है"

रक्षा लेखा प्रधान नियंत्रक) मध्य कमान (1 करियप्पा मार्ग, लखनऊ छावनी226002-
Principal Controller of Defence Accounts (Central Command) 1 Cariappa Road, Lucknow Cantt.– 226002
कार्यालय फोन सं2453038-0522-कार्यालय फ़ैक्स सं/2451084-0522-.
Office Phone No.-0522-2451084/Office Fax No.-0522-2453038
E.Mail- cda-luck@nic.in

आज़ादी का अमृत महोत्सव

No.: EDP/AN/174/Cyber Security/2022-23 **Important Circular** **Date: 23/03/2023**

To

The **Officer-in-Charge** **All Sections** **(Local)**	**The** **Officer-in-Charge** **All Sub-offices** **under PCDA (CC) Lucknow**

Subject : Responding to Ransomware attacks.

Reference : HQrs Office circular No. Mech/IT&S/810/Cyber Security dated 16/03/2023.

With reference to the HQrs office circular cited under reference, it has been directed to follow the prescribed steps in case of Ransomware attacks:

A. Identify & Isolate:

a) Identify systems which are affected or appear to be affected and isolate the identified systems from the network at the switch level.

b) If it is not feasible to isolate the systems at the switch/network level, isolate the systems by making them offline.

c) Unplug all the external storage and turn off any wireless functionality from the systems.

B. Contain:

a) Identify and secure critical systems by temporarily restricting their access and isolation them from the network as an interim measure.

b) Secure network backups by taking them offline immediately and temporarily disable all remote access to the network.

c) Identify and eliminate all forms and sources of threats and disrupt threat actor activities like suspected IPs and domains and terminate malicious processes and stop malicious files, scheduled tasks etc. from being executed.

C. Hardening:

a) Reset credentials of all the privileged local, VPN and domain accounts.

b) Implement multi-factor authentication wherever possible. Also force domain users to change credentials on every next login.

c) Perform user access review and ensure access to only legitimate users.

d) Close SMB, RDP and other unused ports in the network.

e) Ensure deployment of latest patches on all systems.

f) Deploy custom signatures to endpoint protection and network security tools based on discovered Indicators of compromises (IOCs) and ensure endpoint protection is up-to-date and enabled on all systems.

D. Preserve Artefacts & Sanitise systems:

a) Record basic information like "Ransomware Note" text or image, encrypted file extensions etc.

b) Obtain forensic image and capture memory of affected devices for further analysis and also collect relevant logs.

c) Backup of the infected systems be kept so that in case a decryptor is made available in future, encrypted files could be decrypted.

d) Use updated endpoint protection solutions (AV, EDR, XDR etc.) to sanitise systems. Systems should be only connected to network after ensuring they are infection free.

E. Securely Recover & Resume:

a) Ensure that all the previous vulnerabilities and threats are eliminated and the systems are hardened.

b) Affected systems made be recovered by:-

- Restoring from a secure backup
- Restoring from a previous secure restore point.
- Rebuilding & re-installing from scratch.

c) When secure backups and restore points are not available, and rebuilding of the systems from scratch is the only available option, backups of encrypted critical system data should be taken.

d) After restoration, scan with updated endpoint protection solutions to ensure no residual infections like backdoors etc. and review firewall configurations.

e) Implement proper network segmentation to ensure isolation of various systems, segments & zones.

F. Monitor:

a) Test each system, application and other components.

b) Monitor the alerts from Security Information & Event Management (SIEM) solution, if available.

c) Periodically analyze relevant logs and check for abnormal system behavior.

d) Before fully resuming the systems to their pre-incident level, systems should be thoroughly tested to ensure they are functioning correctly and cyber threat has been neutralized.

3. In view of the above, all sections and sub-offices are advised to ensure strict compliance of the guidelines given above and disseminate these guidelines to all their sections/subordinates for strict compliance. Action taken report may please be forwarded to this office at the earliest.

Accounts Officer (IT&S)

Copy to:-

OA Cell (Local) : for uploading on website.

4/07/23

Accounts Officer (IT&S)